PRESENTATION
Mrs. Shereen Jones, Assistant General Manager
Group Operations and Information Technology
Jamaica National Building Society
to address
THE CYBER SECURITY AND DIGITAL FORENSICS CONFERENCE
The University of the West Indies
Tuesday, October 1, 2013,

PANEL DISCUSSION:
THE IMPACT OF CYBERCRIMES ON BUSINESS AND ECONOMY

Salutations:

- Our Chairman
- Conference Delegates
- Ladies and gentlemen…

INTRODUCTION

In the fourth "**Mission Impossible**," movie, "**Ghost Protocol**," starring Tom Cruise, a raft of technology is deployed; and one can see iPhones that crack door codes; iPads which spy on security guards; wireless intrusion vectors delivered by balloon and hijacked security networks, and so on.

And, while this movie has many entertaining "hacker" moments, it also highlights the need for us all in the field of Information Technology to become increasingly vigilant about new innovations and the impact of cyber crime on business and our society.

My thanks to the **Mona School of Business and Management** for presenting this **Cyber Security and Digital Forensics Conference**' and also for inviting **Jamaica National Building Society** to participate in this

panel discussion, the ***Impact of Cybercrimes on Business and Economy.***

As **Chief Information Technology Officer** at Jamaica National, an organisation with more than one million members, more than 30 branches and MoneyShops and subsidiaries, across the island; as well as, offices in the United Kingdom, the United States of America and Canada; I know that the discussions today will prove to be extremely worthwhile and beneficial.

Cybercrimes are defined as: ***Offences committed with a criminal motive to intentionally harm the reputation of the victim, or cause physical or mental harm, using modern telecommunication networks.***

Modern techie criminals can target your digital information in a variety of ways that you may never realise. The private information on your computer can be accessed by unscrupulous hackers from anywhere in the world. The sensitive email which you just received on your smart phone, or the hour of sexting you engaged in last night, are equally vulnerable to hackers.

As we increasingly store and access information on smart phones and tablets, the threat of cyber crimes against the security of your personal or company information becomes even more prevalent.

In a report, ***Cybercrime Transcends all Borders***, McAfee Worldwide Consulting reports that in 2011, some **75 million unique pieces of malware** were identified on the Internet…**2,000 pieces of malware per day**, and, the **threat to mobile devices** is regarded by McAfee as one of the **top five security risks** in the **next five years**.

Today, I will briefly consider the **impact of cyber crime**; address **three trends** which are affecting businesses; briefly highlight **JNBS and its activities in this area**; and close with some recommendations.

IMPACT OF CYBER CRIME

The role and power of technology has become progressively critical to modern society, because technology provide unique solutions, improve processes and increase efficiencies, so that all of us can better meet our objectives.

The business impacts of cyber crime are extremely serious and include not only the possibility of **loss of revenue**; but, also **loss of productive time**, **loss of innovation**, where information about a company's secret product may be stolen; and, **loss of reputation** for both the organisation and its customers.

In a recent study, ***The Cost of CyberCrime,*** the cost to the economy in the United Kingdom was estimated at 27 billion pounds per annum, with IP theft and espionage accounting for more than half of this sum. Estimates of the costs of cyber crime to the economy in the United States of America have ranged from millions to hundreds of billions. And, the ease of access to and relative anonymity provided by ICT lowers the risk of being caught, while making crimes straightforward to conduct.

In a 2011 statement before the US House Sub-Committee on Financial Institutions and Consumer Credit, Assistant Director, Cyber Division, FBI, addressed cyber threats facing the USA and how the FBI and its partners are working to protect the financial sector and American consumers.

The statement considers a broad range of cyber crimes, and provides examples of specific crimes. From **account takeovers** to **fraudulent monetary transfers** to **phishing emails;** and, the depth and audacity of the cyber criminals are breathtaking and frightening.

In Jamaica, Senior Superintendent Clifford Chambers, addressing the **Joint Select Committee** hearing on amendments to the **Cybercrime Act 2010** in June 2012, noted that, "***There is hardly any offence being committed now without the use of technology***".

In February 2013, in a news story in ***The Jamaica Observer***, experts from the **Organised Crime Investigative Division** reported that deficiencies in the present Cybercrimes Act have made prosecuting criminals who prey on young girls extremely difficult.

The OCID has noted that there are **25 types of cybercrimes** that are "*not properly addressed by the current 2010 Cybercrimes Act*". These include the stealing of confidential information from persons' accounts, secretly for fraudulent use such as:

- Scamming and spamming
- Cyber stalking, or
- Dissemination of obscene materials
- And, data theft...

The chairman of the Joint Select Committee charged with reviewing the Act**, Minister of State, Julian Robinson**, has noted that for the last two years the **Communication, Forensic and Cybercrimes Unit** of the **Jamaica Constabulary Force** dealt with more than **1,700 cases**, however, not all cases are reported to the police.

It was reported that in Jamaica last year, more than **229 sites**, including governmental agencies, tertiary institutions and private companies, were

hacked into, and the CFCU has reported a significant increase in electronic fraud and the use of **credit and debit cards** for criminal activity.

One of the leading cyber fraud detection and prevention companies in the world, **41st Parameter**, reports that the growth of cyber crime stems from the maturation of the criminal digital underground and its industrial approach to cyber crime. The industrialisation of fraud means that financial institutions must ensure vigilance and awareness of the criminal enterprise and its processes.

CYBERCRIME TRENDS

To assist financial institutions to prepare for the threat, 41st Parameter identified five trends in a June 2013 report, ***The Growing Threats of Cyber Crime:***

Today, I will make a few comments about three of these trends.

- One, **Data breaches** by the numbers…
- Two, **Malware**…
- And, three, DDos…

Data Breaches by the Numbers

Industrial fraud thrives on stolen identities, and has led to data breaches.. In April 2013, **Living Social**, a deal-of-the day website, disclosed that more than **50 million records were compromised**. Such

a breach is of real concern as payment data can be stolen. However, another real concern behind the theft of personal data is ***access gained to email addresses, birthdates and passwords, creating opportunities for identify theft.***

At JNBS, we recently introduced new **Swipe Card technology**, to improve service delivery, reduce in-branch waiting; and **increase the security of teller transactions**. The card, branded, **Swipe and Go**, will help to reduce fraud.

JNBS members can access funds easily, as they will **simply swipe the card**, **put in their PIN number**, and the Teller will then manage the movement of funds, *at their request,*

This technology has been introduced by the Society is the **first step in the process of phasing out passbooks** and is one of several initiatives to make ***banking with JNBS seamless and more secure.***

Malware

A second trend with which we must be concerned about is: malware, which is any malicious software created to cause harm, and can be used to impersonate the victim, or gain access to credentials. Criminals can use malware to exploit weak areas of operating systems, applications and websites in order to control, disrupt or steal information.

And, Malware can be delivered by **repacking a trusted app**, embedding malicious links to sites that contain malware, or sending unsolicited text messages, known as **SMiShng**, which prompt users to provide information.

For the average user, malware can cause **slow systems**, **pop-ups** and **spam emails**. However, these obvious signs may mean that unwanted software has been installed and is observing and tracking your behaviour, copying keystrokes and detecting user IDs and passwords. In other words, your computer can be taken control of and illicit or illegal tasks carried out.

For financial institutions who conduct online businesses, the IT department must be vigilant, to ensure that it is able to **minimize, detect and block** attempts to access its systems and customers' data on devices and accounts.

Distributed Denial of Service (DDoS)

A third challenge is **DDoS** attacks or **Distributed Denial of Service** (DDoS) **attacks**, which have recently been in the news. In 2012, a wave of DDoS attacks, termed, ***Operation Ababil***, targeted major American financial institutions in 2012, including the **New York Stock Exchange** and **JP Morgan Chase**. The result was a limited disruption of the targeted websites.

Other DDoS attacks can lead to **increased Call Center activity**, and even more seriously, can divert the institution's attention from other financial crimes. It is claimed that malicious hackers execute more than **7,000 DDos attacks every day**, and all organisations which conduct business online must be prepared to implement solutions to **minimize, detect and block** such attacks.

Jamaica National Building Society

At Jamaica National, we use certain safeguards to ensure that doing business with us safer and more secure. These include education, training, and securing computers, as well as our digital assets.

Education and Training:

JNBS staff members are trained in a number of areas, to help to protect against cyber criminals. These range from **User ID and password** requirements, **PC, laptop and mobile user security**, **incident reporting, internet access guidelines and increasing awareness regarding phishing techniques, social engineering, hoaxes and spam.**

Securing Computers and Equipment

All software is **continuously updated** and **security checks conducted** on all corporate websites and applications on a regular basis.

All critical data is **reliably backed up** and there is an effective process in place to recover data. A **computer security incident response team** is in place to quickly investigate, identify, address and document any security issues that may arise.

At JNBS, we are extremely aware of the necessity to **protect against skimming**, as cyber criminals are creating devices to **mimic the security features of legitimate ATM hardware**. In the US, criminals have even gone to the extent of **infiltrating supply chains**, with some **new ATMs delivered with malware already installed** on the systems.

More?

CONCLUSION

In closing, I believe that much more can be done to create awareness around the theme which we have been considering today, ***Protecting Identify, Banking and Citizen Information Networks."***

Greater awareness on the part of all stakeholders is essential; and can be achieved through conferences and workshops such as this. It is, therefore,

my hope that this conference will become an annual event; and, that the discourse will encourage greater regional collaboration and sharing of facts and statistics about cybercrime.

Secondly, I urge our Government to develop a strategic and integrated response to the threat of cybercrime. The relevant government agencies must deliver strong leadership, development of appropriate policies and allocation of resources, to enable all of us who use technology…to become a strong, world class information and communication technology sector, appropriately protected against the threat of cybercrime.

At the same time, there are some encouraging signs. The recent amendment of the **Cybercrime Act 2010** has increased the prison sentence for offenders to 25 years; and a **Cyber Emergency Response Team** has been created by the **Ministry of Technology**, which will seek to respond to cyber threats and crimes.

Thirdly, companies, in all sectors, must increase their investment in improved cyber security. Sustained modifications to security and risk management practices and the adoption of international best practices are essential as cyber criminals become increasingly sophisticated.

In conclusion, I ask this question: ***Is it a Mission Impossible to prevent Cyber Crimes?*** From my desk in this business…I do not believe

that it is impossible; but, what I do know is that: **It is NOT a one-off activity**. It means **constant awareness**. It demands **aggressive vigilance**. It requires **competent employees**, who are determined to be winners.

In addition, it is critical that a strong partnership be established between government, the private sector and academia, to ensure greater awareness, knowledge and vigilance. And, together, we must seek to minimize, detect and prevent the threat of cyber crimes by these modern day ***Bonnies and Clydes***.

Mrs. Shereen Jones
Assistant General Manager
Group Operations and Information Technology
Jamaica National Building Society
October 1, 2013